09/701456
PCT/US00/26839
Rec'd PCT/PTO 27 NOV 2000

PORT BLOCKING METHOD AND SYSTEM

Field of the Invention:

The invention relates to the protection of data stored in a computer, and more particularly, to data which has been secured and opened by non-secure applications where a high level application or operating system component acts to disable certain system resources in order to protect the security of data.

Background of the Invention:

In computer systems, processes may access many system resources, such as serial ports or connections to the Internet. In a situation in which secured data is being accessed by a non-secured application, a means must be developed by which the non-secured application can be restricted from performing operations which might compromise the security of the data.

It is known to open secure data in a system which is completely isolated from outside communications, which has no connection to means by which an unsecured application may, by accident or sabotage, compromise the secured data. It is also known to open secure data with secure applications, which are known to be free from the risk of accident or sabotage that would compromise the secured data. These solutions prevent the use of popular software applications to open secured data, or the use of a computer which is not disconnected from outside communications, and thereby are limited in their usefulness.

Summary of the Invention:

The invention discloses a port blocking method particularly applicable to a system in which secured data is transmitted to a recipient computer for use with non-secured applications. An illustrative embodiment of the invention comprises performing a security check on a process and blocking calls for use of a port if they come from a process using secured data. The tracking of secured processes may include determining whether and how often a secured process should be allowed to use a port. The security check may include determining whether the process is secured by consulting a secured process list and determining whether the resource should be available to the process requesting use of the resource.

Further disclosed is a port blocking system, secured data transmission system using

port blocking, computer-readable medium programmed to block port use, and a computer configured to block port use.

Description of the Drawings:

The invention is best understood from the following detailed description when read with the accompanying figures.

Figure 1 is an schematic diagram of a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 2 is a flow chart of a port request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(a) is a flow chart of a port open request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(b) is a flow chart of a port close request in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Figure 3(c) is a flow chart of a security check in a computer system operating according to an illustrative embodiment of the port blocking method of the invention.

Detailed Description of the Invention:

The invention disclosed prohibits certain processes from utilizing the port resources of the computer on which they are running. These may be secured processes for example, ones which have opened secure data. In a preferred embodiment of the invention, the status of a process as secured is determined by the processes presence on a list of secured processes.

In a preferred embodiment, as shown in Fig. 1, in a computer 100, a control application 110 runs on the kernel (ring 0) level 120 and applications 130 run on higher levels 140. When applications request access to port 150, control application 110 monitors and handles these access requests.

As shown in Fig. 2, in some computer systems, for example, Microsoft Windows NT and Windows 2000 operating systems, the port monitoring is able to intercept all port-related calls. When a port request is initiated 200, control application (110 in Fig. 1) intercepts that request, and determines the process id 210. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The

process id is used to determine whether the process is secure (not allowed to open a port) 220. If it is secure, the request is blocked at 230. If it is not secure, then the request is passed on to the port 250.

As shown in Fig. 3(a), in some computer systems, for example, Microsoft Windows 95 and 98 operating systems, the port monitoring is able to intercept only open and close calls. In order to ensure that a process which has access to a port does not then become a secure process, a check must be performed on any process which is to become secure. When an open port request is initiated 300, control application (110 in Fig. 1) intercepts that request, and determines the process id 310. The control application (110 in Fig. 1) in a preferred embodiment accesses a list of processes that are not allowed to open a port. The process id is used to determine whether the process is secure (not allowed to open a port) 320. If it is secure, the request is blocked, 330, and the call is tracked 340. If it is not secure, then the request is passed on to the port and the process ID and port handle are tracked 350.

As shown in Fig. 3(b), when a close port request is initiated 360, control application (110 in Fig. 1) intercepts that request, and completes the call 362. Then the process ID and port handle is removed from the database of tracked open ports 364.

In addition to these operations on open port and close port requests, as shown in Fig. 3(c), when a process undergoes the security check which determines whether it will be secured, 370, its process id is checked against the database of tracked open ports 372. If the process has open ports, the process may not be made secure and the security check fails 374, and the security check is completed 376. If the process does not have open ports it will pass the security check and the process id will be added to the list of secured processes 378.

A further illustrative embodiment of the invention is directed to a port blocking system wherein certain processes are restricted from using a port, according to the methods provided herein. Further disclosed is a secured data transmission system having a port blocking component to prohibit certain processes from using a port according to the methods provided herein. Still further disclosed is a computer-readable medium programmed to block port use according to the methods provided herein. Still further disclosed is a computer configured to include a port blocking system to block certain processes from using a port according to the methods provided herein.

The terms "computer", "computer system", or "system" as used herein should be broadly construed to include any device capable of receiving, transmitting and/or using

information including, without limitation, a processor, microprocessor or similar device, a personal computer, such as a laptop, palm PC, desktop or workstation, a network server, a mainframe, an electronic wired or wireless device, such as for example, a telephone, an interactive television, such as for example, a television adapted to be connected to the Internet or an electronic device adapted for use with a television, a cellular telephone, a personal digital assistant, an electronic pager, and a digital watch. In an illustrative example, information is transmitted in the form of e-mail. Further, a computer, computer system, or system of the invention may operate in communication with other systems over a network, such as, for example, the Internet, an intranet, or an extranet, or may operate as a stand-alone system.

While the invention has been described by illustrative embodiments, additional advantages and modifications will occur to those skilled in the art. Therefore the invention in its broader aspects is not limited to specific details shown and described herein. Modifications may be made without departing from the spirit and scope of the invention. Accordingly, it is intended that the invention not be limited to the specific illustrative embodiments but be interpreted within the full spirit and scope of the appended claims and their equivalents.